FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

September 5, 2023

The Honorable Mike Gallagher
U.S. House of Representatives
1211 Longworth House Office Building
Washington, DC 20515

Dear Representative Gallagher:

Thank you for your letter regarding the security risks posed by cellular connectivity modules provided by companies subject to the jurisdiction, direction, or control of the People's Republic of China (PRC) or the Chinese Communist Party (CCP).

Under my leadership, the Federal Communications Commission has focused on network security like never before. Our approach is to "deter, defend, and develop": deter bad actors, defend against untrusted vendors, and develop a market for trustworthy innovation. Pursuant to this this strategy, the Commission has taken significant actions to protect our networks.

Working with our national security colleagues, we revoked the operating authorities of four Chinese state-owned carriers that were providing service in the United States, under Section 214 of the Communications Act. The Circuit Court of Appeals for the District of Columbia Circuit recently upheld this action with regard to two Chinese government-owned carriers, Pacific Networks and ComNet.

Building on this effort, for the first time the Commission has adopted policies to regularly review foreign companies' authorizations to provide telecommunications services in the United States. This will help ensure that any authorization reflects up-to-date national security interests and it not frozen in time when Section 214 approval is granted.

In addition, with the help of Congress, the Commission has launched a first-of-its-kind reimbursement program to remove untrusted network equipment from Huawei and ZTE in our Nation's networks and finance efforts to replace it with secure alternatives.

At the same time, we have worked to support innovation that can help improve network security by diversifying vendor opportunities, including open radio access network technology.

The agency has also set up a new Privacy and Data Protection Task Force to develop policies and take enforcement actions to protect our personal information transiting these networks. Untrusted equipment and vendors in telecommunications networks can put at risk our

national and personal security. This Task Force leverages the technical and legal expertise of all the Commission's bureaus and offices to address these matters under the Communications Act.

On top of this, the Commission has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Our rules expressly prohibit the use of federal funds to purchase equipment on this list, which is known as the Covered List. But the list does more than that—it provides all companies making purchasing decisions clear signals about the security of products in the marketplace. To combat ongoing threats from equipment on the list, the Commission has adapted our equipment authorization program to prohibit authorization of such equipment and keep them out of our networks. The Covered List currently identifies equipment and services from ten Chinese entities and one Russian entity, as well as their subsidiaries and affiliates, as posing an unacceptable national security risk.[1]

Under the Secure and Trusted Communications Networks Act, the Commission can update this list only at the direction of national security authorities, specifically the Department of Homeland Security, Department of Defense, Department of Commerce, the Federal Bureau of Investigation, and the Federal Acquisition Security Council. In other words, the agency cannot update this list on its own. Nonetheless, this has been a cooperative process that has worked well to date. In order to ensure that it continues to do so, it is imperative that we keep our national security colleagues apprised of new concerns, including those you raised regarding connectivity modules and equipment produced by Quectel and Fibocom. That is why I have directed the chiefs of the Public Safety and Homeland Security Bureau and the Office of Engineering and Technology to send letters to each of the authorities enumerated in Secure and Trusted Communications Networks Act with a copy of your letter inquiring about the status of these companies.

I believe the issues you raise with respect to connectivity modules merit continued attention. To this end, the Commission is examining additional steps it should take to protect U.S. networks. In addition to our efforts to prevent equipment on the Covered List from being approved through our equipment authorization process, the agency sought comment on the extent to which certain "component parts" associated with equipment authorized by the agency, if produced by entities identified on the Covered List, should be precluded from authorization because they might also pose an unacceptable risk to national security.[2] As part of this effort, the agency also sought comment on whether the Commission should revoke authorizations of specific Covered List equipment that was issued prior to the date any prohibition on

---

[1] The Covered List currently includes certain telecommunications and video surveillance communications equipment produced by five particular Chinese entities – Huawei, ZTE, Hytera, Hikvision, and Dahua (and their subsidiaries or affiliates). It also includes information security products and services supplied by AO Kaspersky Lab (and its predecessors, successors, parents, subsidiaries, or affiliates) and communications services provided by five entities (China Mobile, China Telecom, China Unicom, Pacific Networks Corp, and ComNet (USA) LLC). *See* https://www.fcc.gov/supplychain/coveredlist.

[2] *Secure Equipment Order and Further Notice*, FCC 22-84, at 110-14 ¶¶ 277-287.

authorization went into effect, what the process would be for doing so, and how this would work in the marketplace. At present, the agency is examining the record in this proceeding and considering what steps will further protect communications networks and equipment supply chains.

With respect to information the Commission has on cellular connectivity modules, the agency's Equipment Authorization System (EAS) identifies entities that have obtained equipment authorizations of cellular modules. Quectel and Fibocom are among those that have obtained authorizations of modules. As a matter of practice, however, the agency does not have information about whether authorized equipment may have been or is currently used in U.S. networks, and, if so, where precisely it is deployed.

Nonetheless, as noted above, we coordinate closely and regularly with our federal partners and executive branch bodies that have the responsibility for making determinations regarding equipment and services that pose an unacceptable risk and have written to them to ensure that this matter receives appropriate review. My office will keep your apprised of the response to the letters we have sent.

Finally, I want you to know that I welcome further discussion to update the law to ensure our Nation's communications networks are secure. In particular, I believe it is vital that Congress support the Commission's effort to remove untrusted network equipment in our Nation's networks and fully fund the reimbursement program administered by the agency. In the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to support the removal of this equipment in our networks. However, this amount falls short of what is required. As I have previously noted to Congress, an additional $3.08 billion is needed to fully fund this program and support the many small and rural carriers that have deployed this equipment and need to replace it in their networks.

I appreciate your interest in this national security matter. Please let me know if I can be of any further assistance.

Sincerely,

Jessica Rosenworcel

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Alan F. Estevez
Under Secretary
Bureau of Industry and Security
Department of Commerce
Room 3876
14th and Constitution Avenue, NW,
Washington, DC 20230

Dear Mr. Estevez:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Chris DeRusha
Chair, Federal Acquisition Security Council
Federal Chief Information Security Officer
Deputy National Cyber Director
725 17th St NW
EEOB 292
Washington DC 20503

Dear Mr. DeRusha:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Iranga Kahangama
Assistant Secretary for Cyber, Infrastructure, Risk and Resilience
Office of Strategy, Policy, and Plans
Department of Homeland Security
245 Murray Lane, SW
Washington, DC 20528-0075

Dear Sir or Madam:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Jeanette J. McMillian
Assistant Director
Supply Chain and Cyber Directorate
National Counterintelligence and Security Center
Office of Director of National Intelligence
1500 Tysons McLean Drive
McLean, VA 22102

Dear Ms. McMillian:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Lee G. Licata
Deputy Chief, Telecommunications and Supply Chain
Foreign Investment Review Section, National Security Division
U.S. Department of Justice
175 N St. NE
Pennsylvania Avenue NW
Washington, D.C. 20002

Dear Mr. Licata:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Margaret N. O'Malley
Assistant General Counsel
National Security & Cyber Law Branch
Federal Bureau of Investigation
935 Pennsylvania Ave NW
Washington, DC 20535

Dear Ms. O'Malley:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Michele T. Iversen
Assistant Director
Director of Risk Assessment and Operational Integration
Chief Information Officer
Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301

Dear Ms. Iversen:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Nora Davis
Chief Operations Officer, Cyber Security Directorate
National Security Agency
9800 Savage Rd.
Fort Meade, MD 20705

Dear Ms. Davis:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

September 5, 2023

The Honorable Raja Krishnamoorthi
U.S. House of Representatives
2367 Rayburn House Office Building
Washington, DC 20515

Dear Representative Krishnamoorthi

Thank you for your letter regarding the security risks posed by cellular connectivity modules provided by companies subject to the jurisdiction, direction, or control of the People's Republic of China (PRC) or the Chinese Communist Party (CCP).

Under my leadership, the Federal Communications Commission has focused on network security like never before. Our approach is to "deter, defend, and develop": deter bad actors, defend against untrusted vendors, and develop a market for trustworthy innovation. Pursuant to this this strategy, the Commission has taken significant actions to protect our networks.

Working with our national security colleagues, we revoked the operating authorities of four Chinese state-owned carriers that were providing service in the United States, under Section 214 of the Communications Act. The Circuit Court of Appeals for the District of Columbia Circuit recently upheld this action with regard to two Chinese government-owned carriers, Pacific Networks and ComNet.

Building on this effort, for the first time the Commission has adopted policies to regularly review foreign companies' authorizations to provide telecommunications services in the United States. This will help ensure that any authorization reflects up-to-date national security interests and it not frozen in time when Section 214 approval is granted.

In addition, with the help of Congress, the Commission has launched a first-of-its-kind reimbursement program to remove untrusted network equipment from Huawei and ZTE in our Nation's networks and finance efforts to replace it with secure alternatives.

At the same time, we have worked to support innovation that can help improve network security by diversifying vendor opportunities, including open radio access network technology.

The agency has also set up a new Privacy and Data Protection Task Force to develop policies and take enforcement actions to protect our personal information transiting these networks. Untrusted equipment and vendors in telecommunications networks can put at risk our

national and personal security. This Task Force leverages the technical and legal expertise of all the Commission's bureaus and offices to address these matters under the Communications Act.

On top of this, the Commission has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Our rules expressly prohibit the use of federal funds to purchase equipment on this list, which is known as the Covered List. But the list does more than that—it provides all companies making purchasing decisions clear signals about the security of products in the marketplace. To combat ongoing threats from equipment on the list, the Commission has adapted our equipment authorization program to prohibit authorization of such equipment and keep them out of our networks. The Covered List currently identifies equipment and services from ten Chinese entities and one Russian entity, as well as their subsidiaries and affiliates, as posing an unacceptable national security risk.[1]

Under the Secure and Trusted Communications Networks Act, the Commission can update this list only at the direction of national security authorities, specifically the Department of Homeland Security, Department of Defense, Department of Commerce, the Federal Bureau of Investigation, and the Federal Acquisition Security Council. In other words, the agency cannot update this list on its own. Nonetheless, this has been a cooperative process that has worked well to date. In order to ensure that it continues to do so, it is imperative that we keep our national security colleagues apprised of new concerns, including those you raised regarding connectivity modules and equipment produced by Quectel and Fibocom. That is why I have directed the chiefs of the Public Safety and Homeland Security Bureau and the Office of Engineering and Technology to send letters to each of the authorities enumerated in Secure and Trusted Communications Networks Act with a copy of your letter inquiring about the status of these companies.

I believe the issues you raise with respect to connectivity modules merit continued attention. To this end, the Commission is examining additional steps it should take to protect U.S. networks. In addition to our efforts to prevent equipment on the Covered List from being approved through our equipment authorization process, the agency sought comment on the extent to which certain "component parts" associated with equipment authorized by the agency, if produced by entities identified on the Covered List, should be precluded from authorization because they might also pose an unacceptable risk to national security.[2] As part of this effort, the agency also sought comment on whether the Commission should revoke authorizations of specific Covered List equipment that was issued prior to the date any prohibition on

---

[1] The Covered List currently includes certain telecommunications and video surveillance communications equipment produced by five particular Chinese entities – Huawei, ZTE, Hytera, Hikvision, and Dahua (and their subsidiaries or affiliates). It also includes information security products and services supplied by AO Kaspersky Lab (and its predecessors, successors, parents, subsidiaries, or affiliates) and communications services provided by five entities (China Mobile, China Telecom, China Unicom, Pacific Networks Corp, and ComNet (USA) LLC). *See* https://www.fcc.gov/supplychain/coveredlist.

[2] *Secure Equipment Order and Further Notice*, FCC 22-84, at 110-14 ¶¶ 277-287.

authorization went into effect, what the process would be for doing so, and how this would work in the marketplace. At present, the agency is examining the record in this proceeding and considering what steps will further protect communications networks and equipment supply chains.

With respect to information the Commission has on cellular connectivity modules, the agency's Equipment Authorization System (EAS) identifies entities that have obtained equipment authorizations of cellular modules. Quectel and Fibocom are among those that have obtained authorizations of modules. As a matter of practice, however, the agency does not have information about whether authorized equipment may have been or is currently used in U.S. networks, and, if so, where precisely it is deployed.

Nonetheless, as noted above, we coordinate closely and regularly with our federal partners and executive branch bodies that have the responsibility for making determinations regarding equipment and services that pose an unacceptable risk and have written to them to ensure that this matter receives appropriate review. My office will keep your apprised of the response to the letters we have sent.

Finally, I want you to know that I welcome further discussion to update the law to ensure our Nation's communications networks are secure. In particular, I believe it is vital that Congress support the Commission's effort to remove untrusted network equipment in our Nation's networks and fully fund the reimbursement program administered by the agency. In the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to support the removal of this equipment in our networks. However, this amount falls short of what is required. As I have previously noted to Congress, an additional $3.08 billion is needed to fully fund this program and support the many small and rural carriers that have deployed this equipment and need to replace it in their networks.

I appreciate your interest in this national security matter. Please let me know if I can be of any further assistance.

Sincerely,

Jessica Rosenworcel

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Alan F. Estevez
Under Secretary
Bureau of Industry and Security
Department of Commerce
Room 3876
14th and Constitution Avenue, NW,
Washington, DC 20230

Dear Mr. Estevez:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Chris DeRusha
Chair, Federal Acquisition Security Council
Federal Chief Information Security Officer
Deputy National Cyber Director
725 17th St NW
EEOB 292
Washington DC 20503

Dear Mr. DeRusha:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Iranga Kahangama
Assistant Secretary for Cyber, Infrastructure, Risk and Resilience
Office of Strategy, Policy, and Plans
Department of Homeland Security
245 Murray Lane, SW
Washington, DC 20528-0075

Dear Sir or Madam:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Jeanette J. McMillian
Assistant Director
Supply Chain and Cyber Directorate
National Counterintelligence and Security Center
Office of Director of National Intelligence
1500 Tysons McLean Drive
McLean, VA 22102

Dear Ms. McMillian:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Lee G. Licata
Deputy Chief, Telecommunications and Supply Chain
Foreign Investment Review Section, National Security Division
U.S. Department of Justice
175 N St. NE
Pennsylvania Avenue NW
Washington, D.C. 20002

Dear Mr. Licata:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Margaret N. O'Malley
Assistant General Counsel
National Security & Cyber Law Branch
Federal Bureau of Investigation
935 Pennsylvania Ave NW
Washington, DC 20535

Dear Ms. O'Malley:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Michele T. Iversen
Assistant Director
Director of Risk Assessment and Operational Integration
Chief Information Officer
Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301

Dear Ms. Iversen:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

September 1, 2023

Nora Davis
Chief Operations Officer, Cyber Security Directorate
National Security Agency
9800 Savage Rd.
Fort Meade, MD 20705

Dear Ms. Davis:

Protecting the security of our nation's critical communications networks is a top priority for the Federal Communications Commission. As you know, protecting all of our Nation's communications networks is a whole of government effort.

The FCC has worked with our national security counterparts to publish and update the first-ever list of communications equipment and services that pose an unacceptable risk to national security. Under the Secure and Trusted Communications Networks Act (STCNA), the FCC updates this list, known as the Covered List, based on determinations made by your organization and other specific national security authorities that certain equipment and services poses an unacceptable risk to national security. That is why the Commission has been actively engaged with you through the interagency process to implement STCNA and to promote our collective national and economic security. It is through our continuous collaboration that we have been able to take affirmative and actionable measures to protect the security of our communications networks and the safety of all Americans.

In that spirit, and by way of follow-up to our previous outreach, we want to share with you a recent letter sent by Representatives Mike Gallagher and Raja Krishnamoorthi of the House Select Committee on the Chinese Communist Party, to Commission leadership. The letter expresses concern about the potential security risks by cellular connectivity modules provided by companies that may be subject to the jurisdiction, direction, or control of the People's Republic of China or the Chinese Communist Party.

We welcome the opportunity to collaborate with you in addressing this threat, including consideration of the inclusion of this equipment from Quectel and Fibocom on the Covered List. Thank you for continued efforts in promoting the security of our Nation's communications networks.

Sincerely,

Debra Jordan
Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission

Ronald T. Repasi
Chief
Office of Engineering and Technology
Federal Communications Commission